(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Patentschrift

(10) DE 195 48 903 C2

(51) Int. Cl.[6]:
G 06 F 12/14
G 06 K 19/073
G 07 F 7/10
H 04 L 9/32

(21) Aktenzeichen: 195 48 903.9-53
(22) Anmeldetag: 28. 2. 95
(43) Offenlegungstag: 29. 8. 96
(45) Veröffentlichungstag der Patenterteilung: 20. 3. 97

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
ORGA Kartensysteme GmbH, 33104 Paderborn, DE

(62) Teil aus: P 195 06 921.8

(72) Erfinder:
Eichinger, Siegfried, 33100 Paderborn, DE; Dietrich, Hanno, 33098 Paderborn, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 28 58 819 C2
DE 26 21 271 A1

(54) Verfahren zur Durchführung eines Geheimcodevergleiches bei einem mikroprozessorgestützten tragbaren Datenträger

(57) Verfahren zur Durchführung eines Geheimcodevergleiches zur Benutzeridentifizierung bei Bearbeitungsvorgängen mit einem mikroprozessorgestützten, tragbaren Datenträger, welcher einen EEPROM-Speicher (Electrically Erasable Programmable Read Only Memory) aufweist, und einem Dateneingabe- und Datenausgabegerät (Terminal) zur Kommunikation mit dem tragbaren Datenträger, wobei der vom Benutzer über das Terminal eingegebene Geheimcode mit dem im tragbaren Datenträger gespeicherten Geheimcode verglichen wird, und bei einem falsch eingegebenen Geheimcode ein Fehlbedienungszähler (FBZ) im EEPROM des tragbaren Datenträgers um eins erhöht bzw. erniedrigt wird, so daß der tragbare Datenträger nach einer vorbestimmten Zahl von Fehlversuchen für eine weitere Kommunikation automatisch gesperrt wird, dadurch gekennzeichnet, daß

a) zu Beginn des Verfahrens der aktuelle Wert des Fehlbedienungszählers in einer RAM-Zelle (Random Access Memory) zwischengespeichert wird,

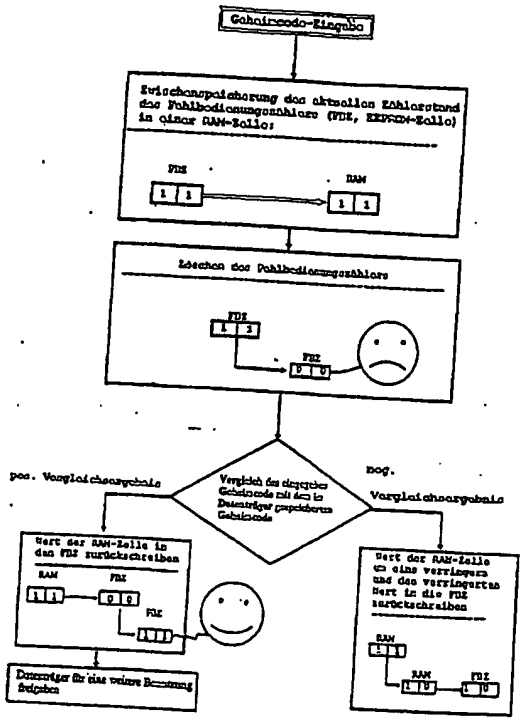
b) nach erfolgter Zwischenspeicherung der Wert des Fehlbedienungszählers (FBZ) auf den vorbestimmten Endwert für die maximale Zahl von Fehlversuchen gesetzt wird,

c) im Anschluß hieran der Geheimcodevergleich durchgeführt wird,

d) bei einem positiven Vergleichsergebnis der jeweilige Wert der RAM-Zelle in den Fehlbedienungszähler zurückgeschrieben wird und der tragbare Datenträger für eine weitere Bearbeitung freigegeben wird,

oder

e) bei einem negativen Vergleichsergebnis der Wert der RAM-Zelle in Richtung auf den vorbestimmten Endwert um eins erhöht oder erniedrigt wird und der geänderte Wert in den Fehlbedienungszähler zurückgeschrieben wird.



DE 195 48 903 C2

DE 195 48 903 C2

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur Durchführung eines Geheimcodevergleiches gemäß dem Oberbegriff des Patentanspruchs.

Eine hierbei verwendete Datenaustauscheinrichtung besteht aus einer Dateneingabe-/Datenausgabegerät (Terminal) und einem mikroprozessorgestützten, tragbaren Datenträger mit einem EEPROM-Speicher (Electrically Erasable Programmable Read Only Memory), insbesondere eine Mikroprozessor-Chipkarte. Jede Transaktion zwischen Terminal und tragbarem Datenträger beginnt mit dem Geheimcodevergleich, welcher zur Überprüfung der Identität des rechtmäßigen Datenträger-Benutzers dient. Der nur dem rechtmäßigen Benutzer bekannte Geheimcode (z. B. die Personal Identification Number, PIN) ist in dem tragbaren Datenträger gespeichert. Der Benutzer gibt den Geheimcode zur Identifizierung über das Terminal ein. Der Vergleich des eingegebenen Geheimcodes mit dem im tragbaren Datenträger gespeicherten Geheimcode erfolgt innerhalb des tragbaren Datenträgers. Vom tragbaren Datenträger wird ein Signal erzeugt, das anzeigt, ob der eingegebene Geheimcode mit dem gespeicherten übereinstimmt oder nicht. Wenn der Geheimcode falsch eingegeben wurde erfolgt ein Hinweis an das Terminal. Die Eingabe des Geheimcodes kann n-mal wiederholt werden, um dem rechtmäßigen Benutzer bei irrtümlich falsch eingegebenen Geheimcodes weitere Identifizierungsversuche zu ermöglichen. Als maximale Zahl von Fehlversuchen wird üblicherweise der Wert drei gewählt. Zu Registrierung der Zahl der Fehlversuche weist der tragbare Datenträger im nicht flüchtigen EEPROM-Speicher einen Fehlbedienungszähler auf. Bei einem falsch eingegebenen Geheimcode wird der Fehlbedienungszähler in Richtung auf den vorbestimmten Endwert für die maximale Zahl von Fehlversuchen je nach Logik um eins erhöht bzw. erniedrigt. Beim Erreichen des vorbestimmten Endwertes wird der tragbare Datenträger dann gesperrt, damit sind weitere Identifizierungsversuche nicht mehr zugelassen.

Ein derartiges Verfahren ist in der DE 2 62 127 A1 beschrieben.

Aufgrund der heutigen Chiptechnologie ist dieses Verfahren allerdings sehr problematisch. Zur Änderung des Fehlbedienungszählers im Fall eines falsch eingegebenen Geheimcodes ist eine Programmierspannung erforderlich, die von einer im tragbaren Datenträger integrierten Ladungspumpe erzeugt wird. Das Ansteuern der Ladungspumpe und der damit zwangsläufig verbundene Anstieg des Versorgungsstromes für den tragbaren Datenträger ist in einfacher und allgemein bekannter Weise extern mittels eines Strommeßgerätes zu detektieren. Für einen mit der Technik vertrauten, unbefugten Benutzer ist es ein leichtes, eine Detektorschaltung zu bauen, die den Start der Ladungspumpe signalisiert und die Ladungspumpe des tragbaren Datenträgers in geeigneterweise stoppt (z. B. durch ein "Ziehen der Reset-Leitung"). Auf diese Weise wird das Setzen des Fehlbedienungszählers wirksam unterbunden. Damit ist die Möglichkeit einer unbegrenzten Zahl von Fehlversuchen gegeben. Durch die damit verbundene indirekte Signalisierung eines falsch eingegeben Geheimcodes, ist es dann möglich den richtigen Geheimcode zu ermitteln. Bei der Verwendung der üblicherweise 4-stelligen PIN als Geheimcode sind hierfür nur maximal 10 000 Versuche nötig, die elektronisch relativ schnell durchzuführen sind.

Zur Lösung dieses Problems wird in der DE 28 58 819 C2 vorgeschlagen, daß das Verhalten des Datenträger nach außen sowohl für Fall eines positiven als auch im Fall eines negativen Geheimcodevergleiches vollständig symmetrisch sein soll. Im negativen Fall wird gemäß der DE 28 58 819 C2 im Fehlbedienungszähler geschrieben; im positiven Fall wird ein Zugriffsbit geschrieben. Damit soll sichergestellt sein, daß die erhöhte Stromaufnahme in beiden Fällen gleich ist, so daß eine Manipulation von außen nicht möglich ist. Ein vollständig symmetrisches Verhalten ist jedoch in der Realität nicht zu erzielen; insbesondere bietet unterschiedliches Zeitverhalten der detektierbaren Stromaufnahmen in den beiden Fällen einen Ansatzpunkt für Betrüger.

Aufgabe der Erfindung ist es daher, ein Verfahren zur Durchführung eines Geheimcodevergleiches zu schaffen, so daß ein optimaler Schutz des tragbaren Datenträgers vor Mißbrauch gewährleistet ist.

Diese Aufgabe wird durch die kennzeichnenden Merkmale des Patentanspruches gelöst.

Zu Beginn des Verfahrens wird der jeweils aktuelle Wert des Fehlbedienungszählers (FBZ) in einer RAM-Zelle (Random Access Memory) zwischengespeichert. Ein Schreib-/Löschvorgang in einer RAM-Zelle ist von außen nicht zu detektieren. Nach erfolgter Zwischenspeicherung wird dann der Wert des Fehlbedienungszählers (FBZ) auf einen vorbestimmten Endwert für die maximale Zahl von Fehlversuchen gesetzt; in diesem Falle der Wert Null. Im Anschluß hieran wird der Geheimcodevergleich durchgeführt. Bei einem positiven Vergleichsergebnis, d. h. Übereinstimmung des eingegebenen Geheimcode mit dem im tragbaren Datenträger gespeicherten Geheimcode, wird der jeweilige Wert der RAM-Zelle in den Fehlbedienungszähler (FBZ) zurückgeschrieben und der Datenträger für eine weitere Bearbeitung freigegeben. Bei einem negativen Vergleichsergebnis wird der Wert der RAM-Zelle um eins verringert, was extern nicht zu detektieren ist, und der verringerte Wert i n den Fehlbedienungszähler (FBZ) zurückgeschrieben. Für einen Betrüger vorteilhafte Manipulationen am Fehlbedienungszähler können nicht vorgenommen werden. Eine Unterbrechung der Stromversorgung hätte eine Sperrung des tragbaren Datenträgers zur Folge.

Patentanspruch

Verfahren zur Durchführung eines Geheimcodevergleiches zur Benutzeridentifizierung bei Bearbeitungsvorgängen mit einem mikroprozessorgestützten, tragbaren Datenträger, welcher einen EEPROM-Speicher (Electrically Erasable Programmable Read Only Memory) aufweist, und einem Dateneingabe- und Datenausgabegerät (Terminal) zur Kommunikation mit dem tragbaren Datenträger, wobei der vom Benutzer über das Terminal eingegebene Geheimcode mit dem im tragbaren Datenträger gespeicherten Geheimcode verglichen wird, und bei einem falsch eingegebenen Geheimcode ein Fehlbedienungszähler (FBZ) im EEPROM des tragbaren Datenträgers um eins erhöht bzw. erniedrigt wird, so daß der tragbare Datenträger nach einer vorbestimmten Zahl von Fehlversuchen für eine weitere Kommunikation automatisch gesperrt wird, **dadurch gekennzeichnet**, daß

a) zu Beginn des Verfahrens der aktuelle Wert des Fehlbedienungszählers in einer RAM-Zel-

Num[illegible] DE 195 48 903 C2
Int. C[illegible] G 06 F 12/14
Veröffentlichungstag: 20. März 1997

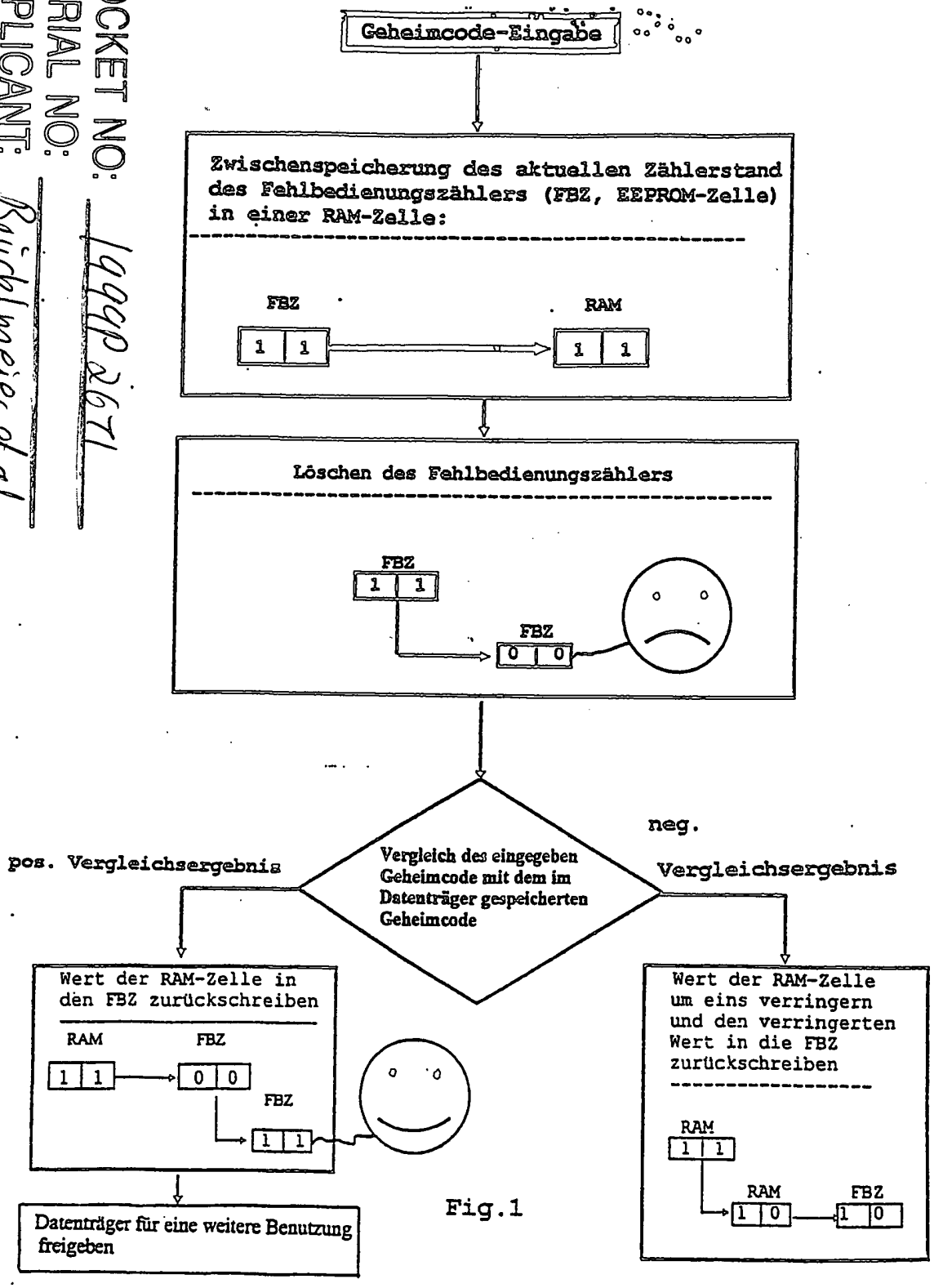


Fig.1